CLAIMS

1. In a distributed network having a number of server computers and associated client devices, method of enforcing an anti-virus security policy, comprising:

querying each of the client devices to determine if each of the client devices has an appropriate anti-virus software installed;

identifying those queried client devices not having the appropriate anti-virus software as target client devices;

locking all communications channels of the target client devices to a anti-virus software installation server; and

installing the appropriate anti-virus software to all target client devices.

2. A method as recited in claim 1, further comprising:

connecting a new client device to the network;

locking all communications channels of the newly connected client device to a anti-virus software installation server; and

installing the appropriate anti-virus software in the newly connected client device.

3. A method as recited in claim 2, wherein the appropriate anti-virus software is determined by a set of policies contained in an operating procedures and policy file.

4. A method as recited in claim 2, further comprising:

posting a notification that the target client devices and the newly connected client devices are prevented from communicating with other systems in the network until such time as the appropriate anti-virus software has been installed therein.

5. A method as recited in claim 2, further comprising:

once the appropriate anti-virus software has been installed in the target client devices or the newly connected client devices,

relinquishing the lock on the communication channels for the newly connected client devices and the target client devices such that the target client devices and the newly connected client devices can communicate with the other devices of network.

6. A method as recited in claim 2, wherein the newly connected client device is a visitor client device.

7. A method as recited in claim 6, further comprising:

determining whether or not the visitor client device is compliant with the appropriate anti-virus software; and

granting a temporary credential for use by the visitor client device when it is determined that the visitor client device is compliant with the appropriate anti-virus software.

8. A method as recited in claim 7, further comprising:

periodically determining validity of the credential.

9. A method as recited in claim 8, further comprising:

invalidating the credential when it is determined to not be valid.

10. A method as recited in claim 7, wherein the credential not valid after a period of time as determined by the granting.

11. In a distributed network having a number of server computers and associated client devices, computer program product for enforcing an anti-virus security policy, comprising:

computer code for querying each of the client devices to determine if each of the client devices has an appropriate anti-virus software installed;

computer code for identifying those queried client devices not having the appropriate anti-virus software as target client devices;

computer code for locking all communications channels of the target client devices to a anti-virus software installation server;

computer code for installing the appropriate anti-virus software to all target client devices; and

computer readable medium for storing the computer code.

12. Computer program product as recited in claim 11, further comprising:

computer code for connecting a new client device to the network;

computer code for locking all communications channels of the newly connected client device to a anti-virus software installation server; and

computer code for installing the appropriate anti-virus software in the newly connected client device.

13. Computer program product as recited in claim 12, wherein the appropriate anti-virus software is determined by a set of policies contained in an operating procedures and policy file.

14. Computer program product as recited in claim 12, further comprising:

computer code for posting a notification that the target client devices and the newly connected client devices are prevented from communicating with other systems in the network until such time as the appropriate anti-virus software has been installed therein.

15. Computer program product as recited in claim a2, further comprising:

computer code for once the appropriate anti-virus software has been installed in the target client devices or the newly connected client devices,

computer code for relinquishing the lock on the communication channels for the newly connected client devices and the target client devices such that the target client devices and the newly connected client devices can communicate with the other devices of network.

16. Computer program product as recited in claim 12, wherein the newly connected client device is a visitor client device.

17. Computer program product as recited in claim 16, further comprising:

computer code for determining whether or not the visitor client device is compliant with the appropriate anti-virus software; and

computer code for granting a temporary credential for use by the visitor client device when it is determined that the visitor client device is compliant with the appropriate anti-virus software.

18. Computer program product as recited in claim 17, further comprising:

computer code for periodically determining validity of the credential.

19. Computer program product as recited in claim 18, further comprising:

invalidating the credential when it is determined to not be valid.

20. Computer program product as recited in claim 17, wherein the credential not valid after a period of time as determined by the granting.